CASE STUDIES: SENSITIVE HEALTH INFORMATION AND HIE

Note: Many state initiatives and RHIOs indicate only that they adhere to HIPAA regulations and applicable state laws.

Case Study 1: Arizona Health-e Connection Roadmap [1]

Arizona's roadmap outlines plans for a statewide information exchange. It presents the following options for the treatment of sensitive health information in its information exchange:

1. **Exclude communicable disease, genetic testing, mental health, and alcohol and substance abuse treatment information to provide greater confidentiality protection for that information.** However, the exchange must examine whether this will be workable, given that this information is integrated throughout medical information held by providers. Moreover, segregating that information means that it may not be available to healthcare providers, which may compromise the quality of care provided to consumers.

2. **Include some sensitive information, but exclude information that has the greatest restrictions on use and disclosure**. For example, the e-health information exchange could include mental health information and communicable disease information (both of which may be disclosed for treatment, payment, quality improvement, research, and public health surveillance), but exclude alcohol and drug abuse treatment information held by federally assisted substance abuse treatment programs and genetic testing information (which may not be disclosed for these purposes without consumer consent).

   This option may be workable, if providers holding genetic testing information and substance abuse treatment information can store that information separately from the e-health information exchange.

3. **Include the special information, but restrict the use of all information in the exchange to comply with the most restrictive laws.** For example, the laws protecting special health information all permit disclosure of the information with consent. The exchange could seek consent to include an individual's information in the exchange, contingent on the individual's agreement to use and disclose all information for certain defined purposes.

   There are substantial downsides to seeking affirmative consent to include e-health information in the exchange, as explored in connection with the first challenge. Moreover, a consumer may wish all of his or her health information to be included in the e-health data exchange except alcohol and drug abuse treatment information; this option would thus force consumers to make a difficult choice between better quality of care and protection of more sensitive information.

[1] Options, descriptions, and discussion taken directly from the Arizona Health-e Connection Roadmap. April 4, 2006. Available online at: http://gita.state.az.us/tech_news/2006/Arizona%20Health-e%20Connection%20Roadmap.pdf

4. **Determine a way to <u>flag information</u> that requires more confidentiality protection.** This would alert providers that there is additional information in the system, but perhaps not allow access to this information without express authorization from the consumer.

5. **Ask the Legislature to <u>amend laws</u> to facilitate the e-health information exchange.** For example, confidentiality laws might be amended so that all information is subject only to the restrictions in the federal HIPAA Privacy Rule. An alternative might be to reduce the amount of information subject to greater confidentiality restrictions.

Case Study 2: HealthInfoNet (Maine) [2]

HealthInfoNet, currently in planning stages, is envisioned as an integrated, clinical information system covering the entire state of Maine. Maine began Phase II (Planning & Development) in mid-2005 and anticipates first stage implementation in 2007.

This stage has a significant consumer component, convening a Consumer Stakeholder Committee to develop a set of recommendations for the network's new governing body. This group is a pre-cursor to a standing Consumer Committee. Recommendations regarding sensitive health information include:

1. **The MHINT system shall ensure that statutory and regulatory restrictions on access, disclosure, and use of electronic health information shall apply to the MHINT system.**

- The MHINT system shall include specific safeguards to insure protection of particularly sensitive electronic health information relating to HIV, substance abuse, mental health, family planning, genetic testing, minors' treatment, and other health information accorded heightened confidentiality.
- The system shall comply with the minimum privacy requirements included in all statutes and regulations relating to these conditions and treatments.
- All individuals and organizations that have access to MHINT data shall be required to demonstrate compliance with HIPAA standards.

2. **The MHINT system shall be guided by standards that are most protective of a consumer's right to confidentiality, privacy, and control of access.**

- All aspects of the MHINT system must be designed with security as a constant priority.
- System security shall be a standing item on the governance entity's meeting agendas.
- System security shall be reviewed and assessed on a regular basis by an independent third party organization; reports shall be shared with the Consumer Committee and full Board of Directors.

[2] Recommendations and sub-bullets taken directly from HealthInfoNet Consumer Stakeholder Committee's Consumer Principles (12/7/05). Available online at: http://www.hinfonet.org/cons_comm.shtml